I. General Remarks Concerning This Response

Claims 1-26 are currently pending in the present application. No claims have been amended, added, or canceled in this response. Reconsideration of the claims is respectfully requested.

II. Summary of Present Invention

A methodology is presented for a network single sign-on (SSO) authentication process using digital certificates. A user has access to protected resources, such as legacy applications, that require verification of a user's authentication data prior to providing access. The user's authentication data is encrypted using the public key of the user, and an attribute certificate containing the encrypted authentication data is generated by an attribute-certificate-issuing authority. When a user requires access to the protected resource, an SSO agent performs an initial authentication process against the user. The SSO agent then retrieves the user's attribute certificate, and for subsequent authentication requests for other protected resources, the SSO agent uses the authentication data from the attribute certificate that corresponds to the targeted protected resource. The SSO agent forwards the required authentication data to the protected resource, and the protected resource then authenticates a user based on the provided authentication data.

III. 35 U.S.C. § 101-Double Patenting

The Office action has rejected claim 1 of the present patent application in an obviousness-type double patenting rejection over claim 1 of U.S. Application Number 09/821,079, "Method and system for public-key-based secure authentication to

distributed legacy applications", filed on 3/29/2001. This rejection is respectfully traversed.

The rejection states in its entirety:

> Claim 1 is rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 1 of U.S. Application No. 09821079. Although the conflicting claims are not identical, they are not patentably distinct from each other because both claims use an attribute certificate to authenticate a user by using the authentication information contained within the attribute certificate.

Applicant strongly disagrees that the claims are not patentably distinct. Applicant notes that MPEP § 804 states the following:

> Since the analysis employed in an obviousness-type double patenting determination parallels the guidelines for a 35 U.S.C. 103(a) rejection, the factual inquiries set forth in Graham v. John Deere Co., 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103 are employed when making an obviousness-type double patenting analysis.
> ...
> Any obviousness-type double patenting rejection should make clear:
> (A) The differences between the inventions defined by the conflicting claims -- a claim in the patent compared to a claim in the application; and
> (B) The reasons why a person of ordinary skill in the art would conclude that the invention defined in the claim in issue is an obvious variation of the invention defined in a claim in the patent.

Hence, an obviousness-type double patenting rejection must fulfill the same requirements as an obviousness rejection that is based on 35 U.S.C. 103(a). Applicant argues that the double patenting rejection fails to provide a *prima facie* case of obviousness. Claim 1 of the present patent application recites:

> 1. A method for an authentication process within a data processing system, the method comprising:
> receiving at a single sign-on (SSO) agent an initial authentication request for a user;
> authenticating the user at the SSO agent for the initial authentication request;
> retrieving by the SSO agent an attribute certificate associated with the user; and

authenticating the user for subsequent authentication requests via the SSO agent using authentication data within the attribute certificate.

In the present patent application, the user's attribute certificate is retrieved by a single-sign-on (SSO) agent in response to the SSO agent successfully performing an authentication operation for the user; as recited in other claims, authentication information for the user within the attribute certificate has been encrypted using a cryptographic key that belongs to the user. Initially, the user is authenticated in some manner, then the information from the attribute certificate is employed for subsequent authentication operations, all of which is assisted by an SSO agent.

In contrast, independent claim 1 of the cited '079 patent application recites:

> 1. A method for an authentication process within a distributed data processing system, the method comprising:
>
> receiving an attribute certificate from a client at a host within the distributed data processing system;
>
> extracting encrypted authentication data from the attribute certificate, wherein the encrypted authentication data was generated by encrypting authentication data with a public key associated with the host;
>
> decrypting the encrypted authentication data to regenerate the authentication data using a private key associated with the host; and
>
> forwarding the authentication data to a controlled resource.

In the other patent application, an SSO agent is not employed, and there are not two phases to the authentication operations, e.g., as claimed in the present patent application in which the user is authenticated without using the information from the attribute certificate and then later by using the information from the attribute certificate. Moreover, the authentication information within the attribute certificate has been encrypted using a cryptographic key of the host instead of the user.

The double patenting rejection merely indicates that claim 1 of the present patent application and claim 1 of the other

patent application contain similar elements. However, the fact that

claims in different patent applications contain similar elements does not provide a basis for issuing a double patenting rejection.

Moreover, the double patenting rejection fails to indicate the differences between the two claims, and the rejection also fails to explain whether or not those differences would have been obvious at the time of the invention. Applicant argues that these differences would not have been obvious variations. For example, the authentication information can only be encrypted once using one cryptographic key. If one were to modify either system to employ a different cryptographic key, the manner in which the attribute certificate was made would need to be modified; this would trigger a series of modifications in each system that has ramifications for the potential uses of the attribute certificate.

Applicant notes that the rejection has not provided a motivational statement for a hypothetical modification of the claims of either patent application to reach the claims of the other patent application; in other words, the rejection fails to have the form of a proper *prima facie* case of obviousness. The rejection merely paraphrases a feature of the patent applications, i.e. "both claims use an attribute certificate to authenticate a user by using the authentication information contained within the attribute certificate". Hence, the rejection fails to explain how it would have been obvious to reach the claimed invention of the present patent application.

With respect to the claims of the present patent application, Applicant respectfully submits that, for these and other reasons, it would not have been obvious for one having ordinary skill in the art to have used the applied patent application to reach the claimed invention. Hence, a rejection of the claims cannot be based upon the cited patent application

to establish a *prima facie* case of obviousness. Therefore, a

rejection of the claims under the judicially-created doctrine of double patenting has been shown to be insupportable in view of the cited patent application, and the claims are patentable over the applied patent application. Applicant respectfully requests the withdrawal of the rejection of the claims.

IV. 35 U.S.C. § 103(a)-Obviousness

The Office action has rejected claims 1, 3, 11, 13, 19, and 21 under 35 U.S.C. § 103(a) as unpatentable over Wood, "Security architecture with environment sensitive credential sufficiency evaluation", U.S. Patent Number 6,691,232 B1, filed 8/05/1999, issued 2/10/2004, in view of Parker, "Access control in a distributed computer system", U.S. Patent Number 5,339,403, filed 4/05/1993, issued 8/16/1994. This rejection is traversed.

Applicant strongly disagrees with the rejection of the claims in the present invention over the applied prior art. The rejection of claims 1, 3, 11, 13, 19, and 21 states in its entirety:

> As per claims 1,3, 11, 13, 19, and 21, Wood teaches use of a certificate for authentication in a single sign on system, (Col. 5, lines 50-65). Wood teaches authenticating the user for subsequent authentication via the certificate, (Col. 6, lines 4- 10).
>
> Wood does not teach an attribute certificate.
>
> Parker teaches an attribute certificate including authentication information, (Col. 1, lines 40-45). Parker teaches a system to approve access by and authenticate by forwarding the attribute certificate to a controlled resource (applications) (Col. 1, lines 45-50). It would be obvious to one of ordinary skill in the art to modify the system of Wood with the certificate of Parker because the certificate is from a trusted secure source.

The rejection relies upon Wood et al. merely for its disclosure of an authentication operation that employs a logon credential,

which may be a digital certificate. However, as noted by the rejection, Wood et al. does not disclose the use of attribute

certificates. The rejection then relies upon Parker for its teaching of an attribute certificate.

The rejection presents an argument as if independent claim 1 of the present patent application merely recites an authentication operation followed by usage of an attribute certificate. In contrast, independent claim 1 recites:

> 1. A method for an authentication process within a data processing system, the method comprising:
> receiving at a single sign-on (SSO) agent an initial authentication request for a user;
> authenticating the user at the SSO agent for the initial authentication request;
> retrieving by the SSO agent an attribute certificate associated with the user; and
> authenticating the user for subsequent authentication requests via the SSO agent using authentication data within the attribute certificate.

In the present patent application, the user's attribute certificate is retrieved by a single-sign-on (SSO) agent in response to the SSO agent successfully performing an authentication operation for the user; as recited in other claims, authentication information for the user within the attribute certificate has been encrypted using a cryptographic key that belongs to the user. Initially, the user is authenticated in some manner, then the information from the attribute certificate is employed for subsequent authentication operations, all of which is assisted by an SSO agent. The rejection ignores these features and fails to address them.

Moreover, the motivational statement in the rejection fails to explain why one would have been motivated to employ the attribute certificates of Parker in the system of Wood et al.. The motivational statement merely states that it would have been obvious "because the certificate is from a trusted secure source". Since every digital certificate is ostensibly created by a trusted secure source, the motivational statement merely

recites a truism. More importantly, the rejection fails to

explain the manner in which the teachings of the two references would be used within a hypothetical combination to form a new system with features from each reference. For example, it is unclear what entity in the system of Wood et al. would obtain, manage, or use the attribute certificates of Parker and/or for what purpose. Thus, one cannot determine whether the incorporation of the usage of attribute certificates as taught by Parker into the system of Wood et al. would benefit the implementation of a hypothetical system based on the system of Wood et al. or whether it would be hinder the intended purpose of the system of Wood et al..

Examiner bears the burden of establishing a *prima facie* case of obviousness

The examiner bears the burden of establishing a *prima facie* case of obviousness based on the prior art when rejecting claims under 35 U.S.C. § 103. *In re Fritch*, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992). Only when a *prima facie* case of obviousness is established does the burden shift to the applicant to produce evidence of nonobviousness. *In re Oetiker*, 977 F.2d 1443, 1445, 24 U.S.P.Q.2d 1443, 1444 (Fed. Cir. 1992); *In re Rijckaert*, 9 F.3d 1531, 1532, 28 U.S.P.Q.2d 1955, 1956 (Fed. Cir. 1993). If the Patent Office does not produce a *prima facie* case of unpatentability, then without more the applicant is entitled to grant of a patent. *In re Oetiker*, 977 F.2d 1443, 1445, 24 U.S.P.Q.2d 1443, 1444 (Fed. Cir. 1992); *In re Grabiak*, 769 F.2d 729, 733, 226 U.S.P.Q. 870, 873 (Fed. Cir. 1985). In response to an assertion of obviousness by the Patent Office, the applicant may attack the Patent Office's *prima facie* determination as improperly made out, present objective evidence tending to support a conclusion of nonobviousness, or both. *In re Fritch*, 972 F.2d 1260, 1265, 23 U.S.P.Q.2d 1780, 1783 (Fed. Cir. 1992).

The applied prior art references clearly fail to disclose at least one feature of the present invention as recited within each independent claim, notwithstanding the obviousness arguments presented by the Office action, thereby rendering the applied prior art references incapable of being used as primary and secondary references as argued by the current rejection.

Moreover, a hypothetical combination of the applied prior art references would also fail to reach the claimed invention of the present patent application. As should be recognized, because the applied prior art references in the rejections fail to disclose the claimed features against which the references were applied, and because the references fail to be combinable to produce these claimed features, the rejection fails to fulfill the requirements of a proper obviousness argument.

Applicant respectfully submits that it would not have been obvious for one having ordinary skill in the art to have used the applied prior art references to reach the claimed invention. Hence, a rejection of the claims cannot be based upon the cited prior art to establish a *prima facie* case of obviousness. Therefore, a rejection of the claims under 35 U.S.C. § 103(a) has been shown to be insupportable in view of the cited prior art, and the claims are patentable over the applied references. Applicant respectfully requests the withdrawal of the rejection of the claims.

V. 35 U.S.C. § 103(a)-Obviousness

The Office action has rejected claims 2, 5, 12, 15, 20, and 23 under 35 U.S.C. § 103(a) as unpatentable over Wood, "Security architecture with environment sensitive credential sufficiency evaluation", U.S. Patent Number 6,691,232 B1, filed 8/05/1999, issued 2/10/2004, in view of Parker, "Access control in a distributed computer system", U.S. Patent Number 5,339,403,

filed 4/05/1993, issued 8/16/1994, and in view of Riggins, "System and

method for using an authentication applet to identify and authenticate a user in a computer network", U.S. Patent Number 6,766,454 B1, filed 7/23/1997, issued 7/20/2004. This rejection is traversed.

The rejection relies on Riggins merely for its teaching of asymmetrical encryption. However, Applicant notes that Riggins fails to disclose at least one feature of the present invention and also fails to remedy the deficiencies of a hypothetical combination of Woods et al. and Parker.

Applicant respectfully submits that it would not have been obvious for one having ordinary skill in the art to have used the applied prior art references to reach the claimed invention. Hence, a rejection of the claims cannot be based upon the cited prior art to establish a *prima facie* case of obviousness. Therefore, a rejection of the claims under 35 U.S.C. § 103(a) has been shown to be insupportable in view of the cited prior art, and the claims are patentable over the applied references. Applicant respectfully requests the withdrawal of the rejection of the claims.

VI. 35 U.S.C. § 103(a)-Obviousness

The Office action has rejected claims 4, 6, 7, 10, 14, 16, 17, 22, 24, and 25 under 35 U.S.C. § 103(a) as unpatentable over Wood, "Security architecture with environment sensitive credential sufficiency evaluation", U.S. Patent Number 6,691,232 B1, filed 8/05/1999, issued 2/10/2004, in view of Parker, "Access control in a distributed computer system", U.S. Patent Number 5,339,403, filed 4/05/1993, issued 8/16/1994, and in view of Olden, "Security and access management system for web-enabled and non-web-enabled applications and content on a computer network", U.S. Patent Number 6,460,141 B1, filed 10/28/1998, issued 10/01/2002. This rejection is traversed.

The rejection relies on Olden merely for its teaching of interfacing with legacy applications. However, Applicant notes that Olden fails to disclose at least one feature of the present invention and also fails to remedy the deficiencies of a hypothetical combination of Woods et al. and Parker.

Applicant respectfully submits that it would not have been obvious for one having ordinary skill in the art to have used the applied prior art references to reach the claimed invention. Hence, a rejection of the claims cannot be based upon the cited prior art to establish a *prima facie* case of obviousness. Therefore, a rejection of the claims under 35 U.S.C. § 103(a) has been shown to be insupportable in view of the cited prior art, and the claims are patentable over the applied references. Applicant respectfully requests the withdrawal of the rejection of the claims.

VII. 35 U.S.C. § 103(a)-Obviousness

The Office action has rejected claims 8, 18, and 26 under 35 U.S.C. § 103(a) as unpatentable over Wood, "Security architecture with environment sensitive credential sufficiency evaluation", U.S. Patent Number 6,691,232 B1, filed 8/05/1999, issued 2/10/2004, in view of Parker, "Access control in a distributed computer system", U.S. Patent Number 5,339,403, filed 4/05/1993, issued 8/16/1994, and in view of Butt, "Certificate-based authentication system for heterogeneous environments", U.S. Patent Number 6,754,829 B1, filed 12/14/1999, issued 6/22/2004. This rejection is traversed.

The rejection relies on Butt merely for its teaching of X.509 digital certificates. However, Applicant notes that Butt fails to disclose at least one feature of the present invention and also fails to remedy the deficiencies of a hypothetical combination of Woods et al. and Parker.

Applicant respectfully submits that it would not have been obvious for one having ordinary skill in the art to have used the applied prior art references to reach the claimed invention. Hence, a rejection of the claims cannot be based upon the cited prior art to establish a *prima facie* case of obviousness. Therefore, a rejection of the claims under 35 U.S.C. § 103(a) has been shown to be insupportable in view of the cited prior art, and the claims are patentable over the applied references. Applicant respectfully requests the withdrawal of the rejection of the claims.

VIII. Conclusion

It is respectfully urged that the present patent application is patentable, and Applicant kindly requests a Notice of Allowance.

For any other outstanding matters or issues, the examiner is urged to call or fax the below-listed telephone numbers to expedite the prosecution and examination of this application.

DATE: September 26, 2006

Respectfully submitted,

Jeffrey S. LaBaw
Reg. No. 31,633
ATTORNEY FOR APPLICANT